

We claim:

1. A method of encryption of data, in which the data is made up of a series of data items, the method including the following steps:
- 5 selecting a chaotic equation from a set of chaotic equations;
defining starting conditions of the variables of the chaotic equation in the form of an input key; and
applying the chaotic equation to each data item.
- 10 2. A method of encryption as claimed in claim 1, wherein the method includes an iterate step of updating the chaotic equation and the input key for each iteration value.
- 15 3. A method of encryption as claimed in claim 2, wherein an updated chaotic equation is applied to each subsequent data item.
- 20 4. A method of encryption as claimed in claim 1, wherein the step of applying the chaotic equation to the data item includes applying a modular arithmetic operation to combine the real and imaginary parts of the result of the chaotic equation and the data item.
- 25 5. A method of encryption as claimed in claim 4, wherein the encrypted data item is defined as $v \equiv (v \text{ xor } |z_{n+1}|) \bmod v_{\max}$, where z_{n+1} is the value of the chaotic equation and v_{\max} is the maximum value of v .
6. A method of encryption as claimed in claim 1, wherein the data is a continuous stream of data items.

7. A method of encryption as claimed in claim 6, wherein the stream of data items has a rate dependency.

8. A method of encryption as claimed in claim 1, wherein the data item is a byte, a word or a dword.

9. A method of encryption as claimed in claim 1, wherein the chaotic equation is one of a group that can comprise: Fractal equations, Julia sets, Lorenz attractor, Rossler attractor, Hénon attractor, Gumowski/Mira attractor and Tinkerbell attractor.

10. A method of encryption as claimed in claim 1, wherein the defined variables of the equation are the key to the encryption and are required at the encrypting source and the decrypting receiver.

11. A method of encryption as claimed in claim 1, wherein the method includes skipping data items by applying the chaotic equation to the data item and discarding the result.

12. A method of encryption as claimed in claim 1, wherein the data items are grouped in blocks with each block having an identifier providing information of the position of the block in the data.

13. A method of encryption as claimed in claim 12, wherein the identifier is not encrypted.

14. A method of encryption as claimed in claim 12, wherein a mask is generated for each block by applying the chaotic equation to each data item in the block.

15. An apparatus for encryption of data, in which the data is made up of a series of data items, the apparatus including:

means for selecting a chaotic equation from a set of chaotic equations;

means for defining starting conditions of the variables of the chaotic

5 equation in the form of an input key; and

means for applying the chaotic equation to each data item.

16. An apparatus as claimed in claim 15, wherein the apparatus includes an
10 iterate means of updating the chaotic equation and the input key for each iteration value.

17. An apparatus as claimed in claim 16, wherein the means for applying the
chaotic equation to the data item applies an updated chaotic equation to each
subsequent data item.

18. An apparatus as claimed in claim 15, wherein the means for applying the
chaotic equation to the data item includes applying a modular arithmetic operation to
combine the real and imaginary parts of the result of the chaotic equation and the data
item.

19. An apparatus as claimed in claim 18, wherein the encrypted data item is
defined as $v = (v \text{ xor } [z_{n+1}]) \bmod v_{\max}$, where z_{n+1} is the value of the chaotic equation
and v_{\max} is the maximum value of v .

20. An apparatus as claimed in claim 15, wherein the data is a continuous stream
of data items.

21. An apparatus as claimed in claim 20, wherein the stream of data items has a rate dependency.

22. An apparatus as claimed in claim 15, wherein the apparatus includes a plurality of defined chaotic equations.

23. An apparatus as claimed in claim 15, wherein the data item is a byte, a word or a dword.

24. An apparatus as claimed in claim 15, wherein the chaotic equation is one of a group that can comprise: Fractal equations, Julia sets, Lorenz attractor, Rossler attractor, Hénon attractor, Gumowski/Mira attractor and Tinkerbell attractor.

25. An apparatus as claimed in claim 15, wherein the defined variables of the equation are the key to the encryption and are required at the encrypting source and the decrypting receiver.

26. An apparatus as claimed in claim 15, wherein the apparatus includes means for skipping data items by applying the chaotic equation to the data item and discarding the result.

27. An apparatus as claimed in claim 15, wherein the data items are grouped in blocks with each block having an identifier providing information of the position of the block in the data.

28. An apparatus as claimed in claim 27, wherein the identifier is not encrypted.

29. An apparatus as claimed in claim 27, wherein a mask is provided for each block by applying the chaotic equation to each data item in the block.

30. A computer program product stored on a computer readable storage medium,
5 comprising computer readable program code means for performing encryption of data made up of a series of data items, including for performing the following steps:

selecting a chaotic equation from a set of chaotic equations;

defining starting conditions of the variables of the chaotic equation as an
input key; and

10 applying the chaotic equation to each data item.

31. A method of detecting unauthorised use of a device comprising:

providing an initial input key for a device;

the device communicating with a server using encrypted data, wherein the
15 input key for the encryption is updated for every data item encrypted;
at the end of a communication, storing the last used input key in a persistent
store in the device and the server;

at the next communication using an iteration of the stored input key.

20 32. A method as claimed in claim 31, wherein the device is a mobile telephone, a smart card or a magnetic stripe card.

33. A method as claimed in claim 31, wherein the encryption method uses a
chaotic equation and the initial input key is the starting conditions of the variables of
25 the chaotic equation.

34. A method as claimed in claim 31, wherein the data items are bytes of data.

35. An apparatus comprising a device and a server with which the device

5 communicates at each use of the device,

the device having an initial input key corresponding to an initial input key in the server;

means for communication between the device and the server using encrypted data, wherein the input key for the encryption is updated for every data item

10 encrypted;

storage means in the device and the server for storing the last used input key in a communication;

the device using an iteration of the stored input key for the next communication.

15

36. An apparatus as claimed in claim 35, wherein the device is a mobile telephone, a smart card or a magnetic stripe card.

37. An apparatus as claimed in claim 35, wherein the means for communication

20 uses encryption based on a chaotic equation and the initial input key is the starting conditions of the variables of the chaotic equation.

38. An apparatus as claimed in claim 35, wherein the data items are bytes of data.

25

20075840-021402